REMARKS

Claims 1-30 are currently pending in the subject application and are presently under consideration. Claims 1, 5, 11, 15, 21, and 25 have been amended as shown on pp. 2-7 of the Reply.

Applicant's representative thanks the Examiner for the courtesies extended during the telephonic interview on July 18, 2007, between Examiners Roderick Tolentino and Gilberto Barron and Applicant's representative Bradley D. Spitz. During the interview, the rejection of claims 1-30 under 35 U.S.C. §103(a) and the cited references relevant to said rejection were discussed. Further, potential amendments to independent claims 1, 5, 11, 15, 21, and 25 were discussed.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-30 Under 35 U.S.C. §103(a)

Claims 1-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Nessett *et al.* (U.S. 6,766,453) in view of Dujari *et al.* (U.S. 7,191,467). Withdrawal of this rejection is requested for at least the following reasons. The cited references, either alone or in combination, do not disclose or suggest all features recited in the subject claims as amended.

> To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *See In re Vaeck,* 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991).

Amended independent claim 1 (and its corresponding dependent claims) recites: *A method for registering a first device with a second device, comprising the steps of: generating a first secret known to the first device and a second secret known to the second device using communications between the first device and the second device over a first communication channel using a first communication method; from the first device, producing first information derived from the first secret; from the second device, producing second information derived from the second secret;* ***using a communication channel other than the first communication channel and a communication method other than the first communication method, comparing the first information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same****; and enabling the first and second device to use the first and second secrets upon the third party being assured that the first secret and the second secret are the same.* The subject amendments are supported by the specification. For example, the specification discloses that a first device can initiate registration with a second device by utilizing and communicating through a wireless network (*see* p. 7, ll. 21-23; p. 21, ll. 4-9). Further, the specification discloses that verification of the registration process can be performed using a different communication method than that used by the registration process, such as by saving registration to a transportable medium or generating a printout of registration information for verification by a network administrator. (*See* p. 5, ll. 14-15; p. 6, ll. 22-23).

Nessett *et al.* relates to techniques for performing an authenticated Diffie-Hellman key agreement protocol over a network where the communicating parties, such as a client device and a wireless network access point, share a secret key with a third party. (*See* col. 2, ll. 40-47). Under the protocol described by Nessett *et al.*, a wireless client system and a network access point transmit a secret key to a third party RADIUS server. (*See* col. 2, ll. 52-57). Once both secret keys have been transmitted, the client system generates a first registration message to the network access point. (*See* col. 2, ll. 58-67). In turn, the network access point generates a second registration message and transmits the first and second messages to the RADIUS server for authentication. (*See* col. 3, ll. 1-11). However, independent claim 1 recites ***using a communication channel other than the first communication channel and a communication method other than the first***

communication method, *comparing the first information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same*. Nessett *et al.* does not disclose or suggest such novel features.

As illustrated by Fig. 2 of Nessett *et al.*, the RADIUS server 250 that performs third-party verification in the process generally described *supra* is located in a common wireless network 200 with the registering network access point AP1 210 and wireless client electronic system WC 220. (*See* col. 5, ll. 61-65; col. 6, ll. 14-18). Thus, the RADIUS server 250 disclosed in Nessett *et al.* uses the same communication method used by the registering access point 210 and client system 220, *i.e.*, communication over the wireless network 200, to verify the registration process. Further, Nessett *et al.* discloses that both Diffie-Hellman variables used in the registration process between the access point 210 and the client system 220 are transferred to the RADIUS server 250 by the access point 210 *via* a single network connection 240. (*See* col. 9, ll. 1-10).

The Examiner additionally relies on Dujari *et al.* at Page 3 of the Office Action; however, Dujari *et al.* does not overcome the deficiencies noted *supra*. Dujari *et al.* generally relates to techniques for providing extended functionality for Internet browsers in order to facilitate authentication between an Internet client and a server *via* a third party authentication service. (*See* abstract; col. 6, ll. 46-65). As described by Dujari *et al.*, a client can initiate a request for communication with a server by sending an unauthenticated request to the server. (*See* col. 13, ll. 59-67). The server can then require third party authentication of the client by responding to the client's request with a server challenge. (*See* col. 14, 1-6). The client then obtains third party authentication by communicating with a third party login server. (*See* col. 17, ll. 43-47, 65-67). More specifically, the client collects user credentials, such as a username and password, and communicates these credentials to a login server. (*See* col. 18, ll. 51-63). The credentials are then evaluated by the login server, which authenticates the client upon determining that the supplied user credentials are valid. (*See* col. 19, ll. 34-39).

The Examiner asserts at Page 3 of the Office Action that Dujari *et al.* teaches using a communication channel other than the first communication channel, comparing the first information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same; and enabling the first device

and second device to use the first and second secrets upon the third party being assured that the first secret and the second secret are the same. However, like Nessett *et al.*, Dujari *et al.* is silent as to ***using a communication channel other than the first communication channel and a communication method other than the first communication method*** for verifying registration information, as recited by independent claim 1.

As generally described by Dujari *et al.*, a client and a server communicate *via* the Internet using HTTP. (*See* col. 6, ll. 29-31). A server can then request third-party authentication for a client with which the server is communicating by sending a HTTP authentication challenge to the client. (*See* col. 2, ll. 31-47). Upon receiving this authentication challenge, the client then engages in third-party authentication with a login server as described *supra*. The Examiner is correct in noting that Dujari *et al.* discloses "out-of-band" authentication between the client and the third party login server. However, it is apparent from the context of this statement, as well as the remainder of the reference, that the "out-of-band" authentication disclosed by Dujari et al. does not utilize a communication method other than a first communication method as recited by independent claim 1. Instead, Dujari *et al.* discloses that both the initial client-server communication prior to authentication and the third-party authentication between the client and the login server are conducted *via* the Internet using an HTTP-level protocol. (*See* col. 6, ll. 36-39; col. 7, ll. 16-19). Thus, it is apparent that the use of the term "out-of-band" in Dujari *et al.* indicates only that the third-party registration process occurs independently of the server, *e.g.*, "out-of-band" from the server.

Moreover, Dujari *et al.* does not disclose or suggest ***comparing the first information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same*** as recited by independent claim 1. Independent claim 1 recites *a method for registering a first device with a second device*, where the first device generates first information, the second device generates second information, and the first information and the second information are compared by a third party. Thus, the two registering devices generate information that is verified by a third party to complete the registration process. Dujari *et al.*, as noted *supra*, relates to techniques for registering an Internet client with a server. However, once the server

requests third-party authentication, the authentication is performed between the client and the third party login server independently of the server. The server to which the client is to be authenticated performs no actions and provides no information during the third party verification process. Further, after the verification process, the server checks only whether third party authentication has successfully completed; no additional authentication is performed by the server. (*See* col. 15, 42-62). Thus, Dujari *et al.* teaches comparing information provided by a first device and a third party, and not comparing information provided by a first device and a second device as recited by independent claim 1.

Likewise, independent claims 5, 11, 15, 21, and 25 have been amended to recite similar features to those recited by independent claim 1. Thus, Nessett *et al.* and Dujari *et al.*, either separately or in combination, do not teach or suggest all features of independent claims 5, 11, 15, 21, and 25 for the reasons stated above regarding independent claim 1. Accordingly, Applicant's representative respectfully requests that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP1996US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicant's undersigned representative at the telephone number below.

Respectfully submitted,
Amin, Turocy & Calvin, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

Amin, Turocy & Calvin, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731